

CHAPTER 2

ACCESS AND SECURITY

Section 2A—PURPOSE AND OVERVIEW.

2.1. Chapter Summary. This Chapter focuses on the how to access the new Air Force Supply Central Database (AFSCDB) environment and the security measures in place to secure supply data from unauthorized users. It is important to note that the methods, policy, and procedures described in this section are independent of the SBSS environment. This chapter describes how to sign on, the security methods in place, and the role of the User Administrator.

2.2. Overview.

2.2.1. **Section 2A.** Section 2A, Overview, provides an overview of the chapter and outlines the remaining chapters describing the different methods of access and the controls, security in place within the AFSCDB environment, and the new role of the User Administrator.

2.2.2. **Section 2B.** Section 2B, Sign On and Access, concentrates on the different environments the user must successfully access and what level of data visibility individual users may be granted.

2.2.3. **Section 2C.** Section 2C, Security, outlines the Air Force policy on password administration and the methods in place by AFSCDB to protect supply data.

2.2.4. **Section 2D.** Section 2D, User Administrator, defines the role and responsibilities of a new position created within the supply community to manage and account for new users to AFSCDB.

Section 2B—SIGN ON AND ACCESS.

2.3. Section Summary. This section outlines the need for two separate sign on environments and the various levels of data access that may be granted individual users. This section also defines the user identification structure that must be followed when assigning new users to AFSCDB.

2.3.1. **Two Accounts, One System.** Because of the complexity of the AFSCDB system and the various applications used in its configuration, a web graphical user interface screen was designed to serve as a front-end navigator. When a customer signs onto AFSCDB they will actually sign into their web account. If they are an authorized user they will have access and visibility to their Oracle account menu options based on their access permissions.

2.3.2. **Seamless Sign-On.** Although the user must sign on to two systems, only one user identification name and password will be used. Your web account and Oracle account user identification will be identical and only the Oracle account will be password-protected.

2.4. Web Access.

2.4.1. A user must have a web account established to view the AFSCDB graphical user interface sign in screen. Without an established web account a user is considered an unauthorized user and will not proceed beyond the sign-on screen.

2.4.2. Once a user successfully signs on the user is presented a menu page. This menu page provides links to the various applications and features available to AFSCDB users. This front-end module will grow as more features are added but the basic format will remain the same.

2.4.3. The options that appear on the menu screen may only be activated and called upon if the user has permissions to use the application / feature. If the user has not been granted permissions to use the area by the User Administrator then the menu option will not open the application.

2.5. Oracle Access.

2.5.1. In addition to the web account a user must be established in Oracle. This user account is different from the web account in that it actually resides on the Air Force Supply Central Database (AFSCDB). Without this Oracle account the web account is useless.

2.5.2. The Oracle account is what actually permits the user to access the supply data and grants permissions to other applications and features within the AFSCDB environment. As more capabilities are added or as users requirements change, the User Administrator will adjust individual user Oracle account to Add, Delete, or Change as required.

2.5.3. Oracle takes advantage of approved Air Force password security policy (outlined in [section 2C](#)). In the event you are locked out of the system due to password violations you will not be granted access until your User Administrator unlocks your account. Contact your User Administrator for more details.

2.6. Access Levels and Permissions.

2.6.1. The design of the AFSCDB permits a user to access some or all accounts. Accessibility to these accounts is based on the permissions granted to a user by the User Administrator at the time of user creation.

2.6.2. The decision of account access should be based on the type of work a user performs and if there is a genuine need to view multiple accounts. The number of people granted full Air Force level views should be limited to those that need it in the performance of their duties.

2.6.3. All accounts are controlled and accessed by SRAN. A user may be limited to a single SRAN or given access to multiple SRANS. The distinct advantage of this is that the user may now retrieve data from multiple SRANS with a single integration request.

2.6.4. In addition to Accessing different accounts it is also possible to limit what applications may be used by an individual. The User Administrator will activate and deactivate which applications a user needs in the performance of their duties. Based on this selection the application may be accessed from the web account main menu.

2.7. User Identification Structure.

2.7.1. To assist in user profiling, user analysis, report authoring, user base reconciliation, and user account information, there is a standard format to follow when creating new users to AFSCDB. All User Administrators will follow the guidance outlined below when creating a new user identification name to AFSCDB.

2.7.2. User Identification Naming Conventions:

Position 1-2 Site Identification Code

Position 3-4 Major Command Code

Position 5-8 Unique identifier determined by responsible User Administrator (see User Administrator for detailed information)

AFMAN 23-110 Volume 2

Part 8, Chapter 2

Table 2.1. Base Assignment.

SITE CODES			
CODE	LOCATION	CODE	LOCATION
AA	ANKARA AB, TURKEY	AO	ARAXOS AB, GREECE
AB	ALBROOK AFS, ROP	AR	ARNOLD AFB, TN
AD	ANDERSEN AFB, GUAM	AS	ASCENSION, AFRICA (AFSITE)
AF	ARLINGTON, VA (AF BASE CONVERSION AGENCY)	AT	ALTUS AFB, OK
AG	ALASKA ANG	AV	AVIANO AB, ITALY
AI	HQ AIR INTELLIGENCE AGENCY, SAN ANTONIO, TX	A1	ALABAMA HRO
AJ	AL JABAR, SAUDI ARABIA	A6	ALEXANDRIA, VA (SEC6)
AL	RAF ALCONBURY, ENGLAND	A7	ALPENA, MI ANG
AM	AMHERST AS, NH	A8	ATLANTIC CITY, NJ ANG
AN	ANDREWS AFB, MD	A9	AMARC, AZ
BA	BANGOR, ME ANG	BL	BALTIMORE, MD ANG
BC	BATTLE CREEK, MI ANG	BN	RAF BENTWATERS, ENGLAND
BD	BRADLEY, CT ANG	BO	BOLLING AFB, DC
BE	BEALE AFB, CA	BR	BROOKS AFB, TX
BF	BYRD FIELD, VA ANG	BS	GOWEN FIELD, ID ANG
BG	BERGSTROM AFB, TX	BT	BRIDGETON, MO ANG
BH	BIRMINGHAM, AL ANG	BU	BUCKLEY AFB, CO
BI	BITBURG AB, GERMANY	BV	BURLINGTON, VT ANG
BK	BARKSDALE AFB, LA		
		B1	BARNES, MA ANG
		CT	USCENTAF (SHAW AFB)
CA	SACRAMENTO, CA (HQ CALIFORNIA ANG)	CN	CANNON AFB, NM
CB	CAPE CANAVERAL AFS, FL	CO	COLUMBUS AFS, MS
CC	CHEYENNE MOUNTAIN AFS, CO	CP	CPSC AMMES
CD	CAPE COD AFS, MA	CS	CHARLESTON, WV ANG
CE	CHARLOTTE, NC ANG	CV	CAVALIER AFS, ND
CG	ILSC CHAMBERSBURG, PA	CW	CARSWELL JRB, TX
CH	CHARLESTON AFB, SC	CY	CHEYENNE, WY ANG
CI	CHANNEL ISLAND, CA ANG	CZ	DFAS COLUMBUS
CK	RAF CHICKSANDS, ENGLAND	C1	CLEAR AS, AK
CL	CHARLESTON, SC (FIELD ORGANIZATION)	C2	CHRISTCHURCH, NZ (OPER DF)

AFMAN 23-110 Volume 2
Part 8, Chapter 2

CM	COMISO, AS ITALY		C4	SCOTT AFB (AFCA)
DA	DAVIS MONTHAN AFB, AZ		DO	DOVER AFB, DE
DB	DOBBINS ARB, GA		DT	DAYTON, OH (FIELD ORGANIZATION)
DC	DCC (NETHERLANDS)		DU	DULUTH, MN ANG
DE	DENVER, CO (DSA-DE & DFAS-DE SYSTEM TESTERS)		DY	DYESS AFB, TX
DF	DEFENSE MAPPING AGENCY (ST LOUIS)		D1	HQ AFPC (PERSONNEL APPLICATION SOFTWARE DEVELOPMENT)
DG	DIEGO GARCIA, INDIAN OCEAN		D2	D.C. ANG (113 AW)
DM	DES MOINES, IA ANG		D3	HQ AFPC FUNCTIONAL SYSTEM TESTING/TRAINING
DN	DANNELLY FIELD, AL ANG			
ED	EDWARDS AFB, CA		EK	EARICKSON AS, AK
EF	ELMENDORF AFB, AK		EL	ELLSWORTH AFB, SD
EG	EGLIN AFB, FL		ET	ELLINGTON FIELD, TX ANG
EH	EINSIEDLERHOF AS, GERMANY		EU	DFAS EUROPE (FIELD ORGANIZATION)
EI	EIELSON AFB, AK			
FA	FAIRCHILD, WA ANG		FS	FORT SMITH, AR ANG
FB	FORT BELVOIR, VA		FT	FORT WORTH JOINT RESERVE BASE (NAS)
FC	FAIRCHILD AFB, WA		FW	FORT WAYNE, IN ANG
FD	FLYINGSDALE, ENGLAND		FX	FT DIX, NJ
FE	FE WARREN AFB, WY		FY	FORT RILEY, KS
FL	FALCON AFB, CO (formerly) SHRIVER (new)		F1	FORT CAMPBELL, KY (AF COMMUNICATION RADAR PERSONNEL)
FM	FORT MEAD, MD		F2	FORT LEONARD WOOD, MS
FN	FINEGAN, GUAM (NAS)		F3	FORT CARSON, CO
FO	FORBES FIELD, KS ANG		F5	FORT HOOD, TX
FR	FRESNO, CA ANG			
GA	SSO MONTGOMERY, AL		GN	DECC-DETACHMENT MONTGOMERY, AL
GC	RAF GREENHAM COMMON, ENGLAND		GO	GOODFELLOW AFB, TX
GD	GEORGIA ANG, GA		GP	GULFPORT ANG, MS
GF	GRAND FORKS AFB, ND		GR	GRIFFIS, NY

AFMAN 23-110 Volume 2

Part 8, Chapter 2

GG	GUAM ANG	GS	GRISSOM ARB, IN
GI	GEILENKIRCHEN AB, GERMANY	GU	MAFB-GUNTER ANNEX, AL
GM	GREAT FALLS, MT ANG	GW	GENERAL MITCHELL ARS, MILWAUKEE, WI
HA	HANSCOM AFB, MA	HM	HOMESTEAD ARB, FL
HE	HELLENIKON AB, GREECE	HO	HOLLOMAN AFB, NM
HF	HECTOR FIELD, ND ANG	HQ	HQ USAF
HG	HAWAII ANG	HS	SATO CANO AB, ROH
HH	HAHN AB, GERMANY	HU	HURLBURT FIELD, FL
HI	HICKAM AFB, HI	HW	HOWARD AFB, ROP
HK	HANCOCK FIELD, NY ANG	HY	HENSLEY FIELD, SD ANG
HL	HILL AFB, UT	H2	HQ AFSOC (HURLBURT FLD)
ID	INDIANAPOLIS, IN (DFAS)	IT	ISTRES AB, FRANCE
IN	INCIRLIK AB, TURKEY	IW	IOWA ANG
IO	INDEPENDENT OVERSIGHT (DODIG, AFAA, etc.)	IZ	IZMIR AB, TU
IR	IRAKLION GREECE		
JA	JACKSON, MS ANG	JP	JAPAN (FIELD ORGANIZATION)
JF	JOE FOSS FD, SD ANG	JV	JACKSONVILLE, FL ANG
KA	KADENA AB, JAPAN	KN	KNOXVILLE, TN ANG
KB	KLEINE BROGEL AB, BELGIUM	KO	KOREAN (FIELD ORGANIZATION)
KC	KANSAS CITY (FIELD ORGANIZATION)	KP	KAENA POINT, HI
KE	KEESLER AFB, MS	KR	KIRTLAND AFB, NM
KF	KEFLAVIK AS, ICELAND	KS	KUNSAN AB, ROK
KG	KINGSLEY FIELD, OR ANG	KU	KULIS ANGB, AK
		KW	KWANG JU AB, ROK
KJ	KWAJALEIN, ROMI	KY	KEY FIELD, MS ANG
KL	KELLY AFB, TX	K1	KELLY AFB, TX AFRES
KM	McCONNELL, KS ANG	K2	KELLY AFB, TX ANG
LA	LANGLEY AFB, VA	LM	LIMESTONE (FIELD ORGANIZATION)
LC	ACC REGIONAL SUPPLY SQUADRON	LO	LSSC ST LOUIS, MO
LD	LONG ISLAND, NY ANG	LR	LITTLE ROCK AFB, AR
LG	LITTLE ROCK, AR ANG	LS	LOS ANGELES AFB, CA

AFMAN 23-110 Volume 2
Part 8, Chapter 2

LH	RAF LAKENHEATH, ENGLAND	LU	LUKE AFB, AZ
LI	LINCOLN, NE ANG	LW	LAWTON, OK / LOWRY, CO *
LJ	LAJES FIELD AB, PORTUGAL	LX	LEXINGTON, KY (FIELD ORGANIZATION)
LK	LACKLAND AFB, TX	LY	LINDSEY, AS GERMANY
LL	LAUGHLIN AFB, TX	L2	LANGLEY (X2 SYSTEM)
MA	MANSFIELD, OH ANG	MQ	MCCHORD AFB, WA
MB	MORBACH, GERMANY	MR	MARCH ARB, CA
MC	MCCONNELL AFB, KS	MS	MISAWA AB, JAPAN
MD	MACDILL AFB, FL	MT	MITCHELL FIELD (NAS)
ME	MEMPHIS, TN ANG	MU	MCENTIRE ANGB, SC
MF	MOFFETT FIELD, CA (NAS)	MV	MARTINSBURG, WV ANG
MG	MCGUIRE AFB, NJ	MW	MADISON, WI (TRUAX FLD)
MH	MOUNTAIN HOME AFB, ID	MX	MAXWELL AFB, AL
MI	RAF MILDENHALL, ENGLAND	M1	MINN-ST PAUL ARS, MN
MJ	KEY FIELD ANGB MERIDIAN, MS	M2	MINN-ST PAUL, MN ANG
MK	MILWAUKEE, WI ANG	M3	MORON AB, SPAIN
ML	MCCLELLAN AFB, CA	M4	MUNIZ, PUERTO RICO ANG
MM	MALMSTROM AFB, MT	M5	MEMPHIS, TN (FIELD ORGANIZATION)
MN	MINOT AFB, ND	M7	MAUI, HI (SPACE SURV)
MO	MOODY AFB, GA	M8	MARCH ANG, CA
MP	MIDDLETOWN, PA ANG		
NA	NASHVILLE, TN ANG	NL	NELLIS AFB, NV
NC	NEW CASTLE, DE ANG	NM	NEW MEXICO ANG
NE	NEWARK, OH (COOF)	NN	NEW ORLEANS JRB, LA
NF	NIAGARA FALLS ARS, NY	NO	NEW ORLEANS, LA ANG
NG	NATIONAL GUARD READINESS CENTER	NP	NAPLES, ITALY (NAS)
NJ	FORT MONMOUTH, NJ	NR	NORFOLK, VA (FIELD ORGANIZATION & NAS)
NI	NATICK, MA ANG	NS	NEW BOSTON AFS, NH
NK	NORTH KINGSTON, RI ANG	NW	NEWARK, NJ (FIELD ORGANIZATION)
OA	OAKHANGER, UK	OM	OMAHA, NE (FIELD ORGANIZATION)
OC	DECC OKLAHOMA CITY, OK	ON	ONIZUKA AFS, CA
OF	OFFUTT AFB, NE	OR	ORLANDO, FL (FIELD ORGANIZATION)

AFMAN 23-110 Volume 2

Part 8, Chapter 2

OG	DECC OGDEN, UT		OS	OSAN AB, ROK
OH	ILLINOIS ANG		OT	OTIS ANGB, MA
OK	OAKLAND, CA (FIELD ORGANIZATION)			
PA	PATRICK AFB, FL		PN	PETERSON AFB, CO
PB	PACAF REGIONAL SUPPLY SQUADRON		PO	PORTLAND, OR ANG
PC	HONOLULU, HI (FIELD ORGANIZATION)		PP	POPE AFB, NC
PD	PORTLAND ARS, OR		PR	PEORIA, IL ANG/ PUERTO RICO*
PE	PEASE ANG, NH		PS	PENSACOLA, FL (FIELD ORGANIZATION)
PG	PENTAGON		PT	PITTSBURGH ARS, PA
PH	PHOENIX ANG, AZ /PEARL HARBOR*		PV	PLEASANTVILLE, NJ ANG
PI	PRINCE SULTAN AB, KSA		PX	PATUXENT RIVER, MD (NAS DFAS)
PK	PIRINCLIK AS, TURKEY		P0 thru P4	PACAF DEPLOYED UNITS
PL	PLATTSBURGH AFB, NY		P5 thru P9	PACAF RSS COLLOCATED OPERATING BASES
QA	HQ SSG QUALITY ASSURANCE			
RA	RAMSTEIN AB, GERMANY		RM	RHEIN MAIN AB, GERMANY
RB	DECC-DETACHMENT WARNER ROBINS, GA		RN	RENO, NV ANG
RC	ROCK ISLAND, IL (FIELD ORGANIZATION)		RO	ROBINS AFB, GA
RD	RANDOLPH AFB, TX		RP	ROTA, SPAIN (NAS)
RE	REESE AFB, TX		RR	ROME, NY (FIELD ORGANIZATION)
RH	HQ AFRES, ROBINS AFB GA		RT	RANTOUL, IL (FIELD ORGANIZATION)
RI	RICKENBACHER ANGB, OH		R1	AF OFFICE OF SCIENTIFIC RESEARCH
RL	ROME LABS, NY		R2	RHODE ISLAND HRO
RQ	HQ USAFE			
SA	SAN ANTONIO, TX		SR	STEWART, NY ANG
SB	SERGEANT BLUFF, IA ANG		SS	ST LOUIS, MO ANG
SC	SCOTT AFB, IL		ST	STANDIFORD FIELD, KY ANG
SD	SANDSTON, VA ANG		SU	SUWON AB, ROK

AFMAN 23-110 Volume 2
Part 8, Chapter 2

SE	SEMBACH AB, GERMANY	SV	SAN VITO AS, ITALY/ DECC- DETACHMENT DENVER, CO*
SF	SELFRIDGE ANGB, MI	SX	SCOTIA, NY ANG
SG	SPANGDAHLEM AB, GERMANY	SY	SEYMORE JOHNSON AFB, NC
SH	SHAW AFB, SC	S1	SAN DIEGO, CA (FIELD ORGANIZATION)
SI	SPRINGFIELD, IL ANG	S2	SEASIDE, CA (FIELD ORGANIZATION)
SJ	ST JOSEPH, MO ANG	S3	ST LOUIS, MO (FIELD ORGANIZATION)
SK	SAN ANTONIO, TX (FIELD ORGANIZATION)	S4	DECC-DETACHMENT SAN ANTONIO, TX
SL	SALT LAKE CITY, UT ANG	S5	SCORRO, NM (STF)
SM	SAN BERNARDINO, CA (FIELD ORGANIZATION)	S6	SUFFOLK NY, ANG
SN	SAVANNAH, GA ANG	S7	SOLA SEA AB, NORWAY
SO	SOESTERBERG, GERMANY	S8	REPUBLIC OF SINGAPORE
SP	SHEPPARD AFB, TX	S9	AMC REGIONAL SUPPLY SQUADRON
SQ	SPRINGFIELD-BECKLEY, OH ANG		
TA	TAEGU AB, ROK	TO	TORREJON AB, SPAIN
TC	CAMP MURRAY, TACOMA WA	TR	TRAVIS AFB, CA
TD	TOLEDO, OH ANG	TS	TASZAR AB, HUNGARY
TG	THULE AB, GREENLAND	TU	TUCSON, AZ ANG
TH	TERRE HAUTE, IN ANG	TY	TYNDALL AFB, FL
TI	TINKER AFB, OK	TZ	TUZLA AB, BOSNIA- HERZEGOVINA
TL	TULSA, OK ANG		
UA	USAF ACADEMY, CO	UN	HQ USAFE NON-APPROPRIATED FUNDS (NAF)
UC	HQ USAFE CORE AUTOMATED MAINTENANCE SYS- TEM (CAMS)	UR	USAFE REGIONAL SUPPLY SQUADRON
UH	RAF UPPER HEYFORD, ENGLAND	US	UNIFORMED SERVICES UHS
VA	VANCE AFB, OK	VI	VIRGIN ISLAND/ST. CROIX
VB	VANDENBERG AFB, CA	VL	VOLKEL AB, NETHERLANDS
VF	VOLK FIELD, WI ANG	VN	VAN NUYS, CA
VG	USA USSDC FT LEE, VA		

AFMAN 23-110 Volume 2

Part 8, Chapter 2

WA	WASHINGTON, DC	WM	WOOMERA AS, AUSTRALIA
WC	DOD, INSPECTOR GENERAL	WN	TACOMA, WA (HQ WASHINGTON AIR NATIONAL GUARD)
WD	WASHINGTON, DC	WO	WESTOVER ARB, MA
WE	WESTFIELD, MA ANG	WP	WRIGHT-PATTERSON AFB, OH
WF	US SOLDIER'S AND AIRMAN'S HOME	WR	WILL ROGERS ANGB, OK
WG	WILLOW GROVE ARS, PA	WW	WAHIAWA, HI (NAS)
WH	WHITEMAN AFB, MO	W0	LANGLEY AFB ANG (DEPLOYED TO PRINCE SULTAN, SAUDI ARABIA)
WJ	OFFICE OF PERSONNEL MGMT.	W1	LANGELY AFB ANG (DEPLOYED TO AL JABAR, SAUDI ARABIA)
WK	U.S. INFORMATION AGENCY	W4	WHITEMAN, KS (42 AFR)
WL	RAF WELFORD, ENGLAND		
YG	YOUNGSTOWN ARS, OH	YO	YOKOTA AB, JAPAN
ZA	ZARAGOSA, SPAIN	ZW	ZWEIBRUCKEN, GERMANY

Table 2.2. MAJCOM Codes.

CODE	DESCRIPTION
0B	US Air Force Academy
0D	US Air Forces in Europe
0I	Air Reserve Personnel Center
0J	Air Education and Training Command (AETC)
0M	Air Force Reserve
0N	Headquarters USAF
0R	Pacific Air Forces
0U	Air Intelligence Agency
0V	Air Force Special Operations Command
0Y	Air Force Communications Agency (AFCA)
00	NATO Airborne Early Warning (NAEW) E-3A Component
07	AF Office of Special Investigations
09	USAF Military Personnel Center
1C	Air Combat Command
1F	United States Ammunition Control Point (USAF-ACP)
1L	Air Mobility Command
1M	Air Force Materiel Command
1S	HQ Air Force Space Command

2H	Air Force Combat Operations Staff
2I	Air National Guard Support Center
2L	Air Force Technical Application Center
3X	USCENTAF
4Z	Air National Guard
4I	Joint Communication Support Element (JCSE)

Section 2C—SECURITY.

2.8. Overview. AFSCDB operates under the security direction of DOD 5200.28-STD, “Trusted Computer System Evaluation Criteria.” AFSCDB hardware security resources will operate in accordance with approved Defense Information Systems Agency (DISA) security requirements, and evolve to the C2 level security requirements. AFSCDB has a System Security Authorization Agreement (SSAA) on file and has met the security requirements outlined by the AF Communication community. This section outlines specific security features that may be of interest to the supply community.

2.9. Secure Socket Layer (SSL).

2.9.1. All supply traffic passed from the database via AFSCDB will process through a Secure Socket Layer (SSL). As data is passed through the SSL it becomes 128 bit encrypted providing secure supply data. This encrypted data is then passed via the Internet to your Base Network Control Center (firewall) where it is then transferred in a readable format to your PC.

2.9.2. All supply traffic passed from your PC via AFSCDB will process through your BNCC where it will receive 128 Bit Encryption and relay through the Internet to the SSL where it is captured and passed to the Database.

2.9.3. This SSL dedicated to the database is located at DISA Oklahoma City and is the responsibility of the Database Administrators.

2.10. Password Assignment.

2.10.1. Each user that receives an Oracle Account must protect their access by means of an approved password. The Oracle Password policy differs from the SBSS password policies and is more restrictive in its structure. When the User Administrator creates your account you will be granted a generic password. Upon your initial sign-on you will be directed to change your password. Failure to do so will result in a password failure and lock out of the system.

2.10.2. Physical Security. You are responsible for the physical protection of your password. You are prohibited from sharing your password with anyone. You should also memorize your password to avoid having it written down. You should always be conscience of those around you when you type your password on the keyboard and take other precautions as necessary to protect access into our system. It is a violation to leave your terminal open (signed on to an active AFSCDB session and you are physically away from your PC). If you suspect your password has been compromised, change it with the “Change Oracle Password” function and contact your User Administrator.

2.10.3. AFSCDB passwords take full advantage of the Identification and Authentication Procedures outlined in AFMAN 33-223. Some of the features employed are:

2.10.4. Password composition. Use passwords with at least eight alphanumeric characters (upper and lower case) with at least one special character (! % # etc.). Never make a password related to one's own personal identity, history, or environment.

2.10.5. Expiration. Your password will expire at the 90-day point from its creation. You will receive a notice from the system at the 80-day point warning you that your password will expire in 10 days. You will continue to receive this warning each time you sign on informing you that you have X days remaining to change your password. Failure to change your password in the allotted time frame will result in your account being locked and inaccessible. Once a lock out occurs you must contact your User Administrator for assistance.

2.10.6. Password Library. You are encouraged to create a unique password each and every time you establish your password for AFSCDB. A record of your last ten passwords will be maintained to prevent you from using the same series of passwords within a six-month window. If you attempt to reuse a password that is stored as one of your last ten passwords used within the last six months you will be prompted to select another.

2.10.7. Limited Sign-On Attempts. You must pay diligent attention to the mechanics and details of your sign-on routine. You will be permitted 3 attempts to successfully input the correct password. When the third attempt to sign-on fails your account will be locked and inaccessible. You must contact your User Administrator for assistance.

2.11. Password Administration.

2.11.1. The AFSCDB User Administrator has the responsibility to manage and administer the AFSCDB password program IAW AFMAN 33-223 and other security guides as applicable.

2.11.2. User Lockouts. The AFSCDB system has several security features that will cause a user to be locked out and render the account inaccessible. It is the responsibility of the User Administrator to validate and authenticate the user before unlocking their account.

2.11.3. Password Compromise. The User Administrator has the responsibility to change or delete a suspected or confirmed compromised password immediately.

2.11.4. Deleted Accounts. User Administrators must delete active password and password history from accounts where the user has transferred to another account or otherwise been terminated from the AFSCDB system.

2.11.5. Suspended System Access. User Administrator must delete active password and lock down accounts where the users access to the system has been terminated or suspended.

Section 2D—USER ADMINISTRATOR.

2.12. Overview. The Air Force Supply Central Database is a controlled environment that requires users be granted access and receive limited privileges within the environment. The role of the User Administrator was created to serve as trusted agents to grant access rights and permission levels to individual users. This section outlines the User Administrator appointment process, their duties and responsibilities, guidelines on creating new users, and general information on audit requirements.

2.13. Appointment.

2.13.1. MAJCOM Staff. Each Major Command determines at what level they desire to place the responsibility of User Administrator within their accounts. Some MAJCOM's may elect to retain this task at the RSS level where others may want to pass the task down to the base level.

2.13.2. MAJCOM Level-1 Administrator. Each MAJCOM should appoint a primary and an alternate individual to serve as the command level-1 administrators. The command representatives must submit an appointment letter, administrator agreement letter and DD Form 2875 to HQ OSSG/ILS level-1 administrator. The appointment and agreement letters must be updated annually. A new DD Form 2875 is required for new level-1 administrators. The necessary appointment and agreement letters can be obtained from the HQ OSSG/ILS website.

2.13.3. Level-2 Administrator Appointment. MAJCOM level-1 administrators may mandate specific documentation required for their level-2 administrators. At a minimum a DD 2875 is required for the individual. MAJCOM level-1 administrators may dictate the frequency of documentation updates or reviews for level-2 administrators within their command.

2.14. Duties and Responsibilities.

2.14.1. The primary duty of the User Administrator is the creation of new user accounts within the AFSCDB. User Administrators are also charged with updating the user accounts when permissions change and deleting accounts when no longer needed.

2.14.2. It is vital that the User Administrator validate that the new user is, in fact, an authorized user of the system and that a record of the account assignment is maintained. When a new user requests permission to access the AFSCDB, a DD Form 2875 is used to generate the request. The User Administrator must maintain a DD Form 2875 (or equivalent) on file for all new users and active AFSCDB accounts. This is a mandatory requirement and is vital to passing a System Security Audit by DISA.

2.14.3. User Administrators must follow the approved User Identification format. The last four positions are assigned by the individual User Administrators and may be reused as determined locally.

2.14.4. When creating new accounts it will be necessary to identify the level of access the new user requires. The User Administrator must exercise and enforce discipline when granting this permission. If the user's duties do not require access to multiple accounts then only grant single SRAN access. This diligence will enhance the performance of the database and ensure that those with a valid need have unhindered access to data.

2.14.5. Each new account must have permissions assigned to it. This means that the User Administrator must identify which tools and applications the new user is entitled to access and use. Once again care must be taken to ensure those with a need are not encumbered by those with a desire. If a person's job requires them to use reports as a work product then they may be content to use Discoverer Viewer or Oracle Reports. However, if the user's job is to troubleshoot and analyze data they may need the full capabilities of Discoverer. It is up to the User Administrator to help define the user's needs and grant privileges to the tools needed by the user.

2.14.6. Reset Passwords As Required. This routine task should be done with extreme caution. Keep in mind that it may be possible for an unauthorized user to use a valid user's account to gain access and deliberately lock the account so that he may reset it to one of his choosing. A method of validating the user must be accomplished before resetting the member's password.

2.14.7. Conduct routine internal evaluations and self-inspections on user account management to include DD Form 2875 (or equivalent) user file. The recommended minimum is annually. MAJCOMs may mandate the frequency and requirements of the validation. Administrators should validate changes to user information and permissions, inactive accounts for possible deletion, and non-admin users with more than one account assigned. Administrators should utilize a Discoverer query to manage the validation.

2.15. User Creation Policy and Procedures.

2.15.1. All new user requests must begin with the creation of a DD Form 2875 (or equivalent). Enter AFSCDB in block 16 for the system to access and identify access privileges (SRAN(s) access, Database Privilege(s), and Menu Access) in block 19. Also include permissions required by the users.

2.15.2. Only one Oracle account may be granted to a single user. Multiple account assignment is not needed and is not authorized

2.15.3. It is the individual user's responsibility to inform the User Administrator when there is a valid change in the user account status. Once informed of such a change, the User Administrator must adjust as required to fit the needs of the user.

2.16. Access/Authorized User Audits.

2.16.1. The Supply community has the responsibility to administer its own system access and security program. Specific responsibilities include DD Form 2875's maintained by the User Administrators and the compliance of the Identification and Authentication procedures outlined in this publication and AFMAN 33-223.

2.16.2. MAJCOM Level-1 administrators must be capable of producing the DD Form 2875 of all members designated as Level 2 Administrators within their command. Each DD Form 2875 must accurately reflect the level of permission the User Administrator is capable of granting to the user base. They are also responsible for authoring and administering the System Security Authorization Agreement between AFSCDB and the Communication Security Agency.

2.16.3. User Administrators must be capable of producing DD Form 2875's for each member granted access to the AFSCDB within their span of control. Each DD Form 2875 must accurately reflect the access privileges granted and the various permissions accessible by the individual user. They are also responsible for complying with the user account configuration and password administration.

2.16.4. DISA may randomly perform a no notice sample audit on accounts. Documentation compliance is mandatory. Failure to pass a DISA audit will result in a re-audit within 90 days and may result in removal as a User Administrator.

Section 2E—USER MANAGEMENT USERS MANUAL.

2.17. Overview. The User Management is broken down into two main logical sections: New User Creation and Existing User Management.

2.17.1. New User Creation. Used to create a new user in the AFSCDB. Actions that occur during new user creation include simple functions like inputting initial identification information and formally establishing the user on the system. Actions also include more advanced functions like assigning initial user data, database, and application access privileges.

2.17.2. Existing User Management. The day-to-day management of Air Force Supply Central Database (AFSCDB) users previously created. Actions include non-Supply specific actions, like locking/unlocking accounts, resetting passwords, and killing user sessions. Actions also include Supply specific actions, like updating contact information, changing user access privileges, and deleting users.

2.17.3. Each of the above sections, along with associated screens will be discussed in detail in the following pages.

2.18. New User Creation.

2.18.1. New User Creation spans 4 screens:

Screen 1 – Search/Select User

Screen 2 – Initial User Data

Screen 3 – Create User

Screen 4 – Add/Remove User Access Privileges

2.18.2. Screen 1, Search/Select User.

Figure 2.1. Form Layout.

The screenshot displays a web-based form titled "Supply System User Administration". At the top, there is a search section with a text input field labeled "SearchString" and a button labeled "SearchUserTable". Below this is a section titled "Users" containing a table with a single header row: "NewUserName:NewLastName:NewFirstName:NewMiddleInitial". The table body is currently empty. At the bottom of the "Users" section is a button labeled "SelectUser". A status bar at the very bottom shows a "Message:" followed by the text "Welcome to Supply System User Administration area ...".

2.18.3. The Search/Select User Screen is the first screen a User Administrator encounters.

2.18.3.1. There are 6 objects on the User Search Screen.

2.18.3.1.1. Object 1: Input field, "SearchString," for entering a search string used to select user records. The search string can be part or all of any of the following:

Table 2.3. User Account Name Search Fields

User Account Name	Full 8 Positions of the User Account Name
Site ID	Positions 1-2 Positions of the User Account Name
MAJCOM Code	Positions 3-4 of the User Account Name
Last Name	Last Name of the User
First Name	First Name of the User

NOTE: If the mouse cursor is moved over the label, help text about data entry into the “SearchString” field is provided.

2.18.3.1.2. Object 2: Action button, “SearchUserTable,” for initiating a user search based on the input.

2.18.3.1.3. Object 3: Dual purpose, output/input combo box, “Users.”

2.18.3.1.3.1. In the output mode, it displays 2 types of records. First type is the default New User record and will be discussed in detail later. Second type are records which result from a user search. Order in which records are displayed is as follows:

By SiteID

Then By MajComCode

Then By LastName

Then By FirstName

2.18.3.1.3.2. In the input mode, a particular record is selected for further action.

2.18.3.1.4. Object 4: Main menu Icon, used to return to the AFSCDB main menu screen.

2.18.3.1.5. Object 5: Action button, “SelectUser,” displays information about a specific user on Screen 2, or for a new user when the “NewUserAccount” line is selected in object 3.

2.18.3.1.6. Object 6: Output field, “Message:” is for displaying pertinent messages, like welcome messages and/or number of records returned from a user search.

Figure 2.2. Form Usage.

The screenshot shows a web-based form titled "Supply System User Administration". At the top, there is a search section with a text input field labeled "SearchString" and a button labeled "SearchUserTable". Below this is a section titled "Users" which contains a large, empty rectangular area, likely a table or list of users. At the bottom of the form, there is a button labeled "SelectUser" and a message field that displays "Message: Welcome to Supply System User Administration area ...".

2.18.4. Steps For Creating a New User.

2.18.4.1. The first step in creating a new user is to ensure the proposed User Account Name has not been previously assigned. This is done by entering the full User Account Name in Search-String field. Then click the SearchUserTable Button. For user-id format conventions see paragraph above entitled, "User Identification Naming Conventions."

2.18.4.1.1. No records should return in the Users combo box (object 3), as well as a matching message in Message: field. This is because duplicate account names are not allowed. If the account you selected is unassigned you'll receive the message displayed in the Message field on the screen below.

Figure 2.3. Form Usage.

The screenshot shows a web application window titled "Supply System User Administration". At the top, there is a search bar with the text "SearchString" and the value "MX1L2SMC", followed by a button labeled "SearchUserTable". Below this is a section titled "Users" containing a table with one row: "NewUserAccountName:NewLastName:NewFirstName:NewMiddleInitial". Below the table is a button labeled "SelectUser" with a small icon to its left. At the bottom, a message box displays "Message: 0 User Records returned."

2.18.4.2. The next step is to accept the selection of the default NewUserAccount line in the Users list Object by clicking on the SelectUser button. This will take you to the Initial User Data Screen (Screen 2).

Figure 2.4. Screen 2 – Initial User Data Form Layout.

The screenshot shows a web application window titled "Supply System User Administration". It contains a form with the following fields: "UserAccountName", "LastName", "FirstName", "MiddleInitial", "OfficeSymbol", "CommPhone", "DSNPhone", "EMailAddress", "Password", and "ConfirmPassword". There are two buttons at the bottom: "CreateUser" and "Cancel". A message box at the bottom displays "Message: Fill in Required Fields for a New User and Press Create User Button ...".

2.18.4.2.1. Layout of the Initial User Data Screen is fairly straightforward. There are 13 objects on the Initial User Data Screen. Objects 1-10 are basic identification data fields for a new user and include the following:

Table 2.4. Initial User Data Screen – Data Fields.

SCREEN ITEM	TITLE	NOTES
1	User Account Name	1
2	Last Name	
3	First Name	
4	Middle Initial	
5	Office Symbol	
6	Commercial Phone	
7	DSN Phone	
8	Email Address	
9	Password	2,3
10	Confirmed Password	2

NOTES:

1. On-Screen help is provided when the cursor is moved over the label.
 2. On-Screen help is provided when the cursor is moved over the label.
 3. AFSCDB requires a special character in the password. However, the following special characters are invalid and will not be accepted by the Oracle Database: Space or Blank, @, \$, ^, &, `, =, +, \, |, :, ', ", /, >, <.
- 2.18.4.2.2. Remaining objects are Create User action button, Cancel action button, and Message output field.
- 2.18.4.2.3. Create User action button - displays the “Create User” screen (Screen 3) after entry of the user information entered in Fields 1-10.
- 2.18.4.2.4. Cancel action button - returns to the “Search/Select User” screen, (Screen 1). When Screen 1 comes up from a Cancel on this screen, no prior search criteria is displayed because there’s no search criterion for a new user. This behavior is different, because cancel on other screens preserves the prior input user search criteria.
- 2.18.4.2.5. Message output field displays pertinent messages.

Figure 2.5. Form Usage.

2.18.4.3. The next step in creating a user is to fill in required fields. Required fields are those fields with a dark blue outline. The only optional field is the Middle Initial.

2.18.4.3.1. Ensure the UserAccountName field (User-Id) is properly formatted.

2.18.4.3.2. Password and ConfirmPassword fields must be filled in with a string that will pass DISA password check rules. These are matched fields so be careful to enter the same information, or you will receive a reject on the next screen.

2.18.4.3.3. The next step in creating a user is to click on the CreateUser action button. This takes you to the Confirm Create User screen (Screen 3).

Figure 2.6. Screen 3 – Confirm Create User Form Layout.

2.18.4.3.3.1. The layout of the Create User Screen is brief, since most data was entered previously.

2.18.4.3.3.2. There are 7 items on the Create User Screen.

2.18.4.3.3.3. Items 1-4 just display data from the previous screen about the user account to be created.

1. User Account Name

2. Last Name
3. First Name
4. Middle Initial

2.18.4.3.3.4. The ConfirmCreate action button confirms the data is correct and attempts to create an actual user account.

2.18.4.3.3.5. The Cancel action button allows you to cancel creation of a new user account and displays Screen 2. When Screen 2 is displayed from a Cancel on this screen, no prior input information is retained because it is assumed you wish to create another user. If you need to modify erroneous data input about the current user, then you should hit the browser back button at this time. This reloads Screen 2 with the previously entered information for modification.

2.18.4.3.3.6. The Message output field - displays error or completion messages. Messages displayed may be the result of initial checks, like passwords not matching, or the results from the actual user creation attempt after you click on the ConfirmCreate action button. The text in this field will vary, indicating that the user was created successfully, or that the user was unable to be created and why.

Figure 2.7. Form Usage.

UserAccountName	LastName	FirstName	MiddleInitial
MX1L2SMC	CLANTON	SPENCER	

ConfirmCreate Cancel

Message:

2.18.4.4. The next step in creating a user account is to confirm creation by clicking on Confirm Create. This will refresh the screen and display the result in the Message field.

2.18.4.4.1. The Message field will attempt to provide the user a reason for failure if user account creation fails. Screen 3 will no longer display the ConfirmCreate button. This is done to prevent repeated failed attempts to create a user without correcting the invalid information. At this point, a user must click either the Cancel button on this screen or the Back button for their browser to correct the data that caused the user account creation to fail.

2.18.4.4.2. When user creation is successful, then the Message field will display a message stating so. The Add/Remove User Access Privileges screen, (Screen 4) will be displayed after a short period to allow assignment of access privileges to complete the user account creation.

Figure 2.8. Screen 4 – Add/Remove User Access Privileges Form Layout.

2.18.4.4.3. Add/Remove User Access Privileges Screen contains 18 items and is divided into three sections. The left side of each section lists the privileges assigned to the person who is creating the user account. The right side is the privileges assigned to the new user. The heading contains a few fields (User Account Name, Lastname etc.) about the new user.

2.18.4.4.3.1. The Data Visibility section of the screen refers to SRAN(s)/Air Force Base(s) a user is allowed access to in the database.

2.18.4.4.3.1.1. Fields are divided into 2 groups:

Administrator Group (Left Side)	Admin SRAN List drop down menu lists SRANs the administrator has access to and can assign to a user.
------------------------------------	--

AddSRAN action button - adds the selected SRAN to the user list on the right. Allowing access to this SRAN.

User Group (Right Side)	User SRAN List drop down menu – lists those SRANs the user has been previously assigned.
----------------------------	---

RemoveSRAN action button - removes the selected SRAN from the list the user is allowed access.

2.18.4.4.3.2. Database Privileges section of the screen refers to those internal privileges and setups a user needs to access the database objects correctly.

Fields are divided into 2 groups:

Administrator Group (Left Side)	Admin DB Privilege List drop down menu - lists DB Privileges that the Administrator has assigned and can assign to a user.
------------------------------------	--

AddDBPrivilege action button - adds the selected DB Privilege to the user.

User Group
(Right Side)

User DB Privilege List drop down menu - lists
the DB Privileges that the user has assigned.

RemoveDBPrivilege action button - removes a selected DB Privilege from the user.

2.18.4.4.3.3. The Program Visibility section of the screen refers to those programs the user has access to in the normal login menu list.

2.18.4.4.3.3.1. Fields are divided into 2 groups:

Administrator Group
(Left Side)

Admin App List drop down menu - lists
applications that the Administrator has assigned
and can assign to a user.

AddApp action button - adds the selected Application to the list assigned to a user.

User Group
(Right Side)

User App List drop down menu - lists
applications that the user has assigned.

RemoveApp action button - removes the selected application from the list assigned to a user.

2.18.4.4.3.3.2. The Done action button returns you to the Search/Select User screen. The Add and Remove buttons actually apply the changes to the database as soon as they are selected.

2.18.4.4.3.3.3. Cancel action button returns to the Managing an Existing User version of Screen 2 (to be discussed in a future section). This is done because a user account has been created and has only the default assigned (DiscViewer) because the Cancel button was clicked. If the Cancel button on Screen 2 is selected, Screen 1 is displayed without any prior search criteria.

2.18.4.4.3.3.4. The Message output field is for displaying pertinent messages which result from adding or removing SRANs, DB Privileges, or Applications.

Figure 2.9. Form Usage.

Supply System User Administration

UserAccountName LastName FirstName MiddleInitial
 MXIL2SMC CLANTON SPENCER

Data Visibility Admin SRAN List User SRAN List
 All AF MajComs AddSRAN RemoveSRAN

Database Privileges Admin DB Privilege List User DB Privilege List
 DiscPlus AddDBPrivilege RemoveDBPrivilege

Program Visibility Admin App List User App List
 All Menu Groups AddApp RemoveApp

Done Cancel

Message:

2.18.4.4.4. The last step in creating a user is to assign access privileges. There are three categories//types of access privileges:

Data Visibility

Database Privileges

Program Visibility/Menu Groups

2.18.4.4.4.1. Special instructions.

For Administrative users the following features apply:

1. Level 1 User Administrator (UserAdmLv1 Database Privilege) accounts can create, modify, or delete level 1, 2, or 3 user accounts. In addition, User Administrators are automatically granted access to all SRANs.
2. Level 2 User Administrator (UserAdmLv2 Database Privilege) accounts can create, modify, or delete level 3 user accounts only. In addition, User Administrators are automatically granted access to all SRANs.
3. Level 3 User will have no administrator privileges assigned.

2.18.4.4.4.2. To setup Data Visibility select the proper SRAN(s) from the, Admin SRAN List, and click the, AddSRAN, button to add to the users SRAN list. A user may be granted access to one, some, or all SRANs. The preferred method for adding SRANs to a users account is groups (MAJCOMs). It is advantageous for performance purposes to add an entire MAJCOM or ALL AF MAJCOMs and remove (an) individual SRAN(s), if necessary. For example: A user requires access to all AMC accounts, except Travis and Dover. The best method for granting Data Visibility would be 1L MAJCOM (All AMC),

click “Add SRAN”. The next step would be to select 4427 Travis CA and 4497 Dover DE from the “User SRAN List”. Click the “RemoveSRAN” button. This user now has access to all AMC accounts, except 4427 and 4497. This is the preferred method for creating the user in the above scenario for optimum Discoverer performance.

2.18.4.4.2.1. View before adding any SRANs.

Figure 2.10. Screen Image.

The screenshot shows a web interface with a green sidebar on the left containing a 'Data Visibility' icon. The main area has a light blue background. On the left, under 'Admin SRAN List', there is a dropdown menu showing 'All AF MajComs' and an 'AddSRAN' button below it. On the right, under 'User SRAN List', there is an empty dropdown menu and a 'RemoveSRAN' button below it.

2.18.4.4.2.2. View after with All AF MajComs added.

Figure 2.11. Screen Image.

This screenshot is similar to Figure 2.10, but the 'User SRAN List' dropdown menu now contains the text 'All AF MajComs'. The 'AddSRAN' and 'RemoveSRAN' buttons remain in their respective positions.

2.18.4.4.3. To setup Database Privileges, select the proper Database Privilege from the “Admin DB Privilege List” on the left and click the AddDBPrivilege action button.

2.18.4.4.3.1. View before adding any Privileges.

Figure 2.12. Screen Image.

The screenshot shows a web interface with a yellow sidebar on the left containing a 'Database Privileges' icon. The main area has a light blue background. On the left, under 'Admin DB Privilege List', there is a dropdown menu showing 'UserAdmLv1' and an 'AddDBPrivilege' button below it. On the right, under 'User DB Privilege List', there is an empty dropdown menu and a 'RemoveDBPrivilege' button below it.

2.18.4.4.3.2. View after with UserAdmLv1 added.

Figure 2.13. Screen Image.

This screenshot is similar to Figure 2.12, but the 'User DB Privilege List' dropdown menu now contains the text 'UserAdmLv1'. The 'AddDBPrivilege' and 'RemoveDBPrivilege' buttons remain in their respective positions.

2.18.4.4.3.3. You may also select a Database Privilege from the “User DB Privilege List” on the right and click on the RemoveDBPrivilege action button to remove privileges.

2.18.4.4.4.3.4. DiscViewer choice is the minimum access level a user can have and therefore, cannot be removed. If a user no longer requires access simply delete the account.

2.18.4.4.4.3.5. Special Instructions.

If you select UserAdmLvl1 from the left side and add, you will also be adding UserAdmLvl2 -because level 1 includes all level 2 functions.

When the drop down list on the right side contains UserAdmLvl1 & 2 they must be removed in the following order: UserAdmLvl1 then UserAdmLvl2

StdRptExec is required for Quick Run and Batch Run Apps to work properly when program visibility is assigned to a users App list. Selecting StdRptExec from the left side and clicking the AddDBPrivilege button will create the following items on the right side drop down list:

DiscPlus and StdRptExec. When the drop down list on the right side contains StdRptExec and DiscPlus they must be removed in the following order: StdRptExec then DiscPlus

DiscPlus is required for the Create Queries App to work properly when program visibility is assigned to a users App list.

2.18.4.4.4.4. To setup **Program Visibility**, you select the proper App from the **Admin App List** on the left and click the **AddApp** button. This controls the menu items a user sees on left side of the main menu screen after they have logged in.

Figure 2.14. Screen Image.



Figure 2.15. Screen Image.



2.18.4.4.4.4.1. You may also select an App from the User App List and click the RemoveApp button to remove.

2.18.4.4.4.4.2. In the Program Visibility section, three levels of grouping are supported:

All Menu Groups

Which includes all Specific Menu Groups and their Individual

Applications.

A Specific Menu Group

Which includes its Individual Applications

An Individual Application

2.18.4.4.4.3. Adding all but one of the Menu Groups can be accomplished by adding the All Menu Groups from the left side and then removing the single item you don't want the user to have access to on the right side.

2.18.4.4.4.4. Special Instructions.


Extreme caution must be taken when assigning Apps from the Migration Menu Group to a user. Users with Upload or Restart Upload program visibility will be able to start migrations. No special database privilege is required to start or restart migrations.

If assigning Delete Reports App from the Reports Menu Group you must ensure it is assigned in conjunction with View Outputs App. This is because it's only accessible through the View Outputs App.

When removing database privileges you should also remove the applicable applications as well.

2.18.4.4.4.5. The Done action button returns you to the Search/Select User screen when you're finished assigning privileges to the user. Add and Remove buttons actually applied the changes to the database as soon as they were selected.

Figure 2.16. Login Menu List Quick Reference Tables.



Administration		Database Privilege Requirement
User Admin		UserAdmLvl1 or UserAdmLvl2
Migration		
Download Stat		N O N E R E Q U I R E D
Upload Stat		
Upload 704 Stat		
Detailed Errors		
Restart Upload		
Restart 704 Upload		
View All Stats		
Overall View		
Reports		
Quick Run		StdRptExec
Batch Run		StdRptExec
View Outputs		None Required
View Logs		None Required
View All Logs		None Required
Discoverer		
Create Queries		DiscPlus
View Queries		DiscViewer - (Default)

NOTE: Database privileges required to successfully execute items in a user's login menu list.

2.19. Existing User Management. Existing User Management spans 5 screens:

Screen 1 – Search/Select User

Screen 2 – User Data/Admin Actions

Screen 3 – Add/Remove User Access Privileges

Screen 4 – Kill User Sessions

Screen 5 – Delete User

Screen 6 – Search/Select User

2.19.1. Form Layout:

Figure 2.17. Form Layout.

The screenshot displays a web application window titled "Supply System User Administration". At the top, there is a search section with a text input field labeled "SearchString" and a button labeled "SearchUserTable". Below this is a section titled "Users" containing a table with a single header row: "NewUserName:NewLastName:NewFirstName:NewMiddleInitial". The table body is currently empty. At the bottom of the "Users" section, there is a button labeled "SelectUser" next to a small icon. A message bar at the very bottom of the window displays the text: "Message: Welcome to Supply System User Administration area ...".

2.19.1.1. This is the initial screen that's displayed and the functions of this screen are described in the New User Creation section. After entering your search criteria click the SearchUserTable button.

Figure 2.18. Form Layout.

The screenshot shows a web application titled "Supply System User Administration". At the top, there is a search section with a label "SearchString" followed by a text input field containing "MX1L2SMC" and a button labeled "SearchUserTable". Below this is a section titled "Users" containing a table with the following header: "NewUserAccountName:NewLastName:NewFirstName:NewMiddleInitial". The table is currently empty. At the bottom of the "Users" section is a button labeled "SelectUser" with a small icon to its left. A message box at the bottom of the form displays the text: "Message: Welcome to Supply System User Administration area ...".

2.19.1.2. You should get 1 or more records in the “Users” list and a matching message displayed in the Message field below.

Figure 2.19. Figure.

This screenshot shows the same "Supply System User Administration" form as Figure 2.18, but with one record in the "Users" table. The search string "MX1L2SMC" remains in the input field. The table now contains one row with the following data: "MX1L2SMC:CLANTON:SPENCER:". The "SelectUser" button and the message box are still present. The message box now displays: "Message: 1 User Record returned..".

2.19.1.3. If the user that you're looking for appears in the list, click on that user to highlight and then click the SelectUser action button. The User Data/Admin Actions screen (Screen 2) is displayed.

2.19.1.4. Screen 2 – User Data/Admin Actions.

Figure 2.20. Form Layout.

The screenshot shows a web form titled "Supply System User Administration". The form is organized into several sections:

- Header:** A blue bar with the title "Supply System User Administration".
- User Identification Fields:**
 - UserAccountName (highlighted in green), LastName, FirstName, MiddleInitial
 - OfficeSymbol, CommPhone, DSNPhone, EMailAddress
- Action Buttons:** "UpdateUserInfo" and "CancelChanges".
- Tablespace Fields:** DefaultTablespace, TemporaryTablespace.
- Account Status and Password Fields:**
 - AcctStatus (set to "OPEN" in green), LockDate, ExpirationDate, NewPassword, ConfirmPassword.
 - Buttons: "Lock/Open" and "ResetPassword".
- Bottom Action Buttons:** "ChangeAccess", "KillSession", "DeleteUser", "Cancel".
- Message Field:** A text area labeled "Message:" at the bottom.

2.19.1.5. The layout of the User Data/Admin Actions Screen allows accomplishment of seven separate User Administrative functions:

1. Display and Update User Info
2. Display User Tablespace Info
3. Display User Account Status and Lock/Open User Account
4. Display User Password Expiration Date and Reset User Password
5. Link to Change User Access Privileges Screen
6. Link to Kill User Session(s) Screen
7. Link to Delete User Screen

2.19.1.5.1. The Display and Update User Info function allows for displaying and/or updating the basic identification data input when the user was created. Following identification data fields are displayed:

User Account Name

Last Name

First Name

Middle Initial

Office Symbol

Commercial Phone

DSN Phone

Email Address

2.19.1.5.1.1. These fields with the exception of the “UserAccountName” (User-Id) can be changed at any time.

2.19.1.5.1.2. The UpdateUserInfo action button will attempt to update the changed data. Results of a change attempt will be displayed in the Message field at the bottom of the form.

2.19.1.5.1.3. The CancelChanges action button disregards any changes made on this section of the form and restore the original information. Results of a cancellation will be displayed in the Message field. This is not to be confused with the Cancel button at the bottom of the screen which will take you back to the search Search/Select user screen from here.

2.19.1.5.2. Display User Tablespace Info, includes the 2 fields in the second section. Displays two important internal database tablespaces (Default Tablespace and Temporary Tablespace) assigned to the user. These values are important to Administrative personnel because they may be the reason a user’s account doesn’t work properly. No update capability is provided for this information since they seldom change for a user. It may be necessary to delete and reload a user account if they’re in error.

2.19.1.5.3. Display User Account Status and Lock/Unlock User Account, includes the fields on the left side of the 3rd section of the form. As the name suggests, it displays the current status of a user account. Account Status field is color coded as follows:

Green Account is Open and available for use

Red Account is Locked unavailable for use

2.19.1.5.3.1. Accounts can be in locked status for a variety of reasons, such as an expired password, too many failed login attempts, or manually locked by an administrator. If an account is locked the LockDate field will show the date and time when locked status was assigned. Lock/Open action button is for locking or unlocking the user account. The result of such lock/open attempt will be reflected in the account status field, lock date and displayed in the Message field at the bottom of the form.

2.19.1.5.4. Display User Password Expiration Date and Reset User Password includes 3 fields on the right of the third section. First is to display the current user account password expiration date assigned to the user. The date assigned is calculated by using the following:

2.19.1.5.4.1. The date the user was created or the last date the user changed the password. Plus the expiration timeframe assigned by DISA to the standard user profile.

2.19.1.5.4.2. The NewPassword and ConfirmPassword fields allow an administrator to reset a user’s password. Administrator has to enter the data into these fields. Inputs into these fields must match, thus eliminating the possibility of incorrect entry. If the mouse cursor is placed over either label, it will provide help on formatting a password that will be accepted by DISA. ResetPassword button is for initiating a call back to this screen which

will attempt to do a password change based on the input fields. It will also set a flag in a table so that when the user logs in next, he/she will receive a message stating that they need to change their password (to prevent the administrator from knowing a user's password too long). Result of such reset password attempt will be reflected in the Message field.

2.19.1.5.5. The ChangeAccess action button displays the Add/Remove User Access Privileges Screen, (Screen 3).

2.19.1.5.6. The KillSession action button displays the Kill User Sessions Screen, (Screen 4).

2.19.1.5.7. The DeleteUser action button displays the Confirm Delete Screen, (Screen 5).

2.19.1.5.8. The Cancel action button returns to the search screen. Search screen displays the prior search criteria.

2.19.1.5.9. The Message field at the bottom is for displaying pertinent messages, for example, results of updating user info, locking/opening accounts and resetting passwords.

2.19.2. Form Usage. Form use discussion for the User Data/Admin Actions Screen will focus on 4 separate User Admin function are handled on this screen:

Display and Update User Info

Display User Tablespace Info

Display User Account Status and Lock/Unlock User Account

Display User Password Info and Reset User Password

Display and Update User Information screen initially contains data currently stored in the database for the selected user.

Figure 2.21. Figure.

The screenshot displays the 'Supply System User Administration' form. It contains several sections for user information and actions.

UserAccountName	LastName	FirstName	MiddleInitial
MX1L2SMC	CLANTON	SPENCER	

OfficeSymbol	CommPhone	DSNPhone	EMailAddress
ILS	416-9999	596-4154	GUNTER.COM

Buttons: UpdateUserInfo, CancelChanges

DefaultTablespace	TemporaryTablespace
GVREP01_DATA1L	GVREP01_TEMP1L

AcctStatus	LockDate	ExpirationDate	NewPassword	ConfirmPassword
OPEN		NONE		

Buttons: Lock/Open, ResetPassword

Buttons: ChangeAccess, KillSession, DeleteUser, Cancel

Message:

2.19.2.1. To make a change, update those fields (in this example CommPhone and DSNPhone were changed) and click the UpdateUserInfo action button. After this the screen will refresh, database update will be attempted, fields will be reread from the database, and a message displayed. If the change was successful then the screen will display the updated results. If it wasn't, then the changed fields revert back to the original value. In the above example, the change attempt was successful.

2.19.2.2. The Display User Tablespace Information is for display only. They show if the user is assigned to MajCom specific tablespaces, or if the user is assigned to the overall default tablespaces. In the below example, the user is assigned to MajCom 1L tablespaces.

Figure 2.22. Figure.

The screenshot displays the 'Supply System User Administration' window. It contains several sections for user management:

- User Account Information:** Fields for UserAccountName (MX1L2SMC), LastName (CLANTON), FirstName (SPENCER), MiddleInitial (M), OfficeSymbol (ILS), CommPhone (416-4145), DSNPhone (596-4145), and EMailAddress (GUNTER.COM). Buttons for 'UpdateUserInfo' and 'CancelChanges' are present.
- Tablespace Information:** Fields for DefaultTablespace (GVREP01_DATA1L) and TemporaryTablespace (GVREP01_TEMP1L).
- Account Status and Password:** Fields for AcctStatus (OPEN), LockDate, ExpirationDate (NONE), NewPassword, and ConfirmPassword. Buttons for 'Lock/Open', 'ResetPassword', 'ChangeAccess', 'KillSession', 'DeleteUser', and 'Cancel' are included.
- Message Bar:** A message at the bottom states 'Message: Updated User Data for User MX1L2SMC'.

2.19.2.3. The User Account Status and Lock/Unlock User Account section displays the account status for the selected user (currently OPEN).

Figure 2.23. Figure.

Supply System User Administration				
UserAccountName	LastName	FirstName	MiddleInitial	
MX1L2SMC	CLANTON	SPENCER	M	
OfficeSymbol	CommPhone	DSNPhone	EmailAddress	
ILS	416-4145	596-4145	GUNTER.COM	
UpdateUserInfo		CancelChanges		
DefaultTablespace		TemporaryTablespace		
GVREP01_DATA1L		GVREP01_TEMP1L		
AcctStatus	LockDate	ExpirationDate	NewPassword	ConfirmPassword
OPEN		NONE		
Lock/Open		ResetPassword		
ChangeAccess		KillSession	DeleteUser	Cancel
Message: Updated User Data for User MX1L2SMC				

2.19.2.3.1. The Lock/Open action button is used to change the status. If the account status change was successful, the screen will display the updated results. If it wasn't, then the screen will show the status as it was before the change attempt. In the example below, the account status change was successful. Click on the Lock/Open button again to change the account status back.

Figure 2.24. Figure.

Supply System User Administration				
UserAccountName	LastName	FirstName	MiddleInitial	
MX1L2SMC	CLANTON	SPENCER	M	
OfficeSymbol	CommPhone	DSNPhone	EmailAddress	
ILS	416-4145	596-4145	GUNTER.COM	
UpdateUserInfo		CancelChanges		
DefaultTablespace		TemporaryTablespace		
GVREP01_DATA1L		GVREP01_TEMP1L		
AcctStatus	LockDate	ExpirationDate	NewPassword	ConfirmPassword
LOCKED	26-MAR 10:16:03	NONE		
Lock/Open		ResetPassword		
ChangeAccess		KillSession	DeleteUser	Cancel
Message: Locked Account for User MX1L2SMC				

2.19.2.4. Display User Password Info and Reset User Password Account combines both display only info and a simple update capability. The ExpirationDate field on this form should never display “NONE” because this means expiration date feature of passwords is not being enforced. Update of a user’s password may be needed for a variety of reasons, such as forgotten passwords, expired passwords, etc. To update a user’s password, fill the required fields (NewPasssword and ConfirmPassword) and click the ResetPassword action button. If the password change was successful a message is displayed and the ExpirationDate field will be updated. If unsuccessful, the ExpirationDate is not updated and an error message is displayed.

Figure 2.25. Figure.

The screenshot displays the 'Supply System User Administration' window. It contains several sections for user information and actions:

- User Information Section:** Fields for UserAccountName (MX1L2SMC), LastName (CLANTON), FirstName (SPENCER), MiddleInitial (M), OfficeSymbol (ILS), CommPhone (416-4145), DSNPhone (596-4145), and EMailAddress (GUNTER.COM). Buttons for 'UpdateUserInfo' and 'CancelChanges' are present.
- Tablespace Section:** Fields for DefaultTablespace (GVREP01_DATA1L) and TemporaryTablespace (GVREP01_TEMP1L).
- Account Status Section:** Fields for AcctStatus (OPEN), LockDate, ExpirationDate (NONE), NewPassword, and ConfirmPassword. A 'Lock/Open' button is next to the AcctStatus field, and a 'ResetPassword' button is at the bottom right of this section.
- Action Buttons:** A row of buttons including 'ChangeAccess', 'KillSession', 'DeleteUser', and 'Cancel'.
- Message Bar:** A blue bar at the bottom displaying the message: 'Message: Opened Account for User MX1L2SMC'.

NOTE: Password content security standards are enforced by Defense Information Systems Agency (DISA) and are applied when a password change is attempted or a new password is created.

2.19.2.4.1. In the example below, the change password attempt was successful. Message displayed is “Flag set to Force User to Change on Next Login.” This will force the user, on the first login, to change the password. User will be prompted to enter a new password (DISA constraints will apply).

Figure 2.26. Figure.

Supply System User Administration			
UserAccountName	LastName	FirstName	MiddleInitial
MX1L2SMC	CLANTON	SPENCER	M
OfficeSymbol	CommPhone	DSNPhone	EEmailAddress
ILS	416-4145	596-4145	GUNTER.COM
UpdateUserInfo		CancelChanges	
DefaultTablespace		TemporaryTablespace	
GVREP01_DATA1L		GVREP01_TEMP1L	
AcctStatus	LockDate	ExpirationDate	NewPassword ConfirmPassword
OPEN		NONE	
Lock/Open		ResetPassword	
ChangeAccess		KillSession	DeleteUser
Cancel			
Message: Password Reset for User MX1L2SMC. Flag set to Force User to Change on Next login.			




2.19.2.4.2. To go to the Add/Remove User Access Privileges screen (Screen 3), click the ChangeAccess action button.

2.19.2.4.3. To go to the Kill User Sessions screen (Screen 4), click the KillSession action button.

2.19.2.4.4. To go to the Delete User screen (Screen 5), click the DeleteUser action button.

2.19.3. Screen 3 – Add/Remove User Access Privileges

Figure 2.27. Form Layout.

Supply System User Administration			
UserAccountName LastName		FirstName MiddleInitial	
<input type="text"/>		<input type="text"/>	
Data Visibility 	Admin SRAN List <input type="text"/>	User SRAN List <input type="text"/>	
	<input type="button" value="AddSRAN"/>	<input type="button" value="RemoveSRAN"/>	
Database Privileges 	Admin DB Privilege List <input type="text"/>	User DB Privilege List <input type="text"/>	
	<input type="button" value="AddDBPrivilege"/>	<input type="button" value="RemoveDBPrivilege"/>	
Program Visibility 	Admin App List <input type="text"/>	User App List <input type="text"/>	
	<input type="button" value="AddApp"/>	<input type="button" value="RemoveApp"/>	
<input type="button" value="Done"/>		<input type="button" value="Cancel"/>	
Message: <input type="text"/>			

2.19.3.1. Use/Instructions for this screen are located in the New User Creation Section of this document.

Figure 2.28. Screen 4 – Kill User Sessions - Form Layout.

Supply System User Administration

UserAccountName LastName FirstName MiddleInitial

User Sessions

SID	Serial#	Status	CurrentAction	LogonTime	Machine	Terminal	OSUser	OSPID	OSCommand
-----	---------	--------	---------------	-----------	---------	----------	--------	-------	-----------

KillAllSessions KillSelectedSession Cancel

Message:

2.19.4. The Kill User Sessions Screen contains nine fields/input buttons. The user information section displays User Account Name, Last Name, First Name and Middle Initial of the user selected.

The user sessions section contains a dual purpose, output/input combo box. The following information is displayed for each session:

SID

Serial #

Status

Current Action

Login Time

Machine

Terminal

OSUser

OSPID

OSCommand

2.19.4.1. The KillAllSessions action button will attempt to kill all user sessions listed. The KillSelectedSession action button attempts to kill the current selected user session.

2.19.4.2. The Cancel action button displays the User Data/Admin screen (Screen 2). The Message output field is for displaying pertinent messages about the kill requests.

2.19.5. Form Use.

2.19.5.1. The Kill User Session(s) Screen is meant to aid the User Administrator in stopping those user database processes/sessions which are any of the following:

2.19.5.2. Defunct Died but still on the system taking up resources

2.19.5.3. Not DesiredActive but are deemed to be taking too many systems resources

2.19.5.4. Two buttons are provided that allow the User Administrator to kill varying degrees of user sessions. They are located below the User Sessions list.

Figure 2.29. Figure.

The screenshot displays the 'Supply System User Administration' window. At the top, there is a header bar with the title. Below the header, there are input fields for 'UserAccountName', 'LastName', 'FirstName', and 'MiddleInitial'. The values entered are 'MXIL2SMC', 'CLANTON', 'SPENCER', and 'M' respectively. Below these fields is a section titled 'User Sessions' which contains a table with columns: SID, Serial#, Status, CurrentAction, LoginTime, Machine, Terminal, OSUser, OSPID, and OSCommand. The table lists three sessions, all with a status of 'INACTIVE'. Below the table are three buttons: 'KillAllSessions', 'KillSelectedSession', and 'Cancel'. At the bottom of the window is a 'Message' field.

SID	Serial#	Status	CurrentAction	LoginTime	Machine	Terminal	OSUser	OSPID	OSCommand
0010_06852		INACTIVE	UNKNOWN	26-MAR-10:29:43	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1244	1328
0012_02335		INACTIVE	UNKNOWN	26-MAR-10:28:56	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1388	1260
0013_02787		INACTIVE	UNKNOWN	26-MAR-10:29:25	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1424	1224

2.19.5.5. To kill a selected session, select the session from the User Sessions list and click the KillSelectedSession action button. If successful, specific session line in the user sessions section of the screen is updated to a status of “Killed” (if the status was InActive) or the specific session line will disappear altogether (if the status was Active). In addition, the Message field reflects the results of the kill action.

Figure 2.30. Figure.

The screenshot shows the 'Supply System User Administration' window. At the top, the user 'MX1L2SMC CLANTON SPENCER M' is displayed. Below this is the 'User Sessions' table with columns: SID, Serial#, Status, CurrentAction, LogonTime, Machine, Terminal, OSUser, OSPID, and OSCCommand. The table contains three rows. The first row (SID 0010, Serial# 06852) has a status of 'KILLED'. The second row (SID 0012, Serial# 02335) has a status of 'INACTIVE'. The third row (SID 0013, Serial# 02787) has a status of 'INACTIVE'. Below the table are three buttons: 'KillAllSessions', 'KillSelectedSession', and 'Cancel'. At the bottom, a 'Message' field displays 'Killed User Session ... SID:0010 Serial#:06852'.

SID	Serial#	Status	CurrentAction	LogonTime	Machine	Terminal	OSUser	OSPID	OSCommand
0010	06852	KILLED	UNKNOWN	26-MAR 10:29:43	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1244	1328
0012	02335	INACTIVE	UNKNOWN	26-MAR 10:28:56	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1388	1260
0013	02787	INACTIVE	UNKNOWN	26-MAR 10:29:25	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1424	1224

Message: Killed User Session ... SID:0010 Serial#:06852

Figure 2.31. Figure.

The screenshot shows the 'Supply System User Administration' window. At the top, the user 'MX1L2SMC CLANTON SPENCER M' is displayed. Below this is the 'User Sessions' table with columns: SID, Serial#, Status, CurrentAction, LogonTime, Machine, Terminal, OSUser, OSPID, and OSCCommand. The table contains two rows. The first row (SID 0012, Serial# 02335) has a status of 'INACTIVE'. The second row (SID 0013, Serial# 02787) has a status of 'INACTIVE'. Below the table are three buttons: 'KillAllSessions', 'KillSelectedSession', and 'Cancel'. At the bottom, a 'Message' field is empty.

SID	Serial#	Status	CurrentAction	LogonTime	Machine	Terminal	OSUser	OSPID	OSCommand
0012	02335	INACTIVE	UNKNOWN	26-MAR 10:28:56	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1388	1260
0013	02787	INACTIVE	UNKNOWN	26-MAR 10:29:25	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1424	1224

Message:

2.19.5.6. **KillAllSessions** action button kills all sessions for the displayed user. If successful, the specific session lines in the User Sessions section are updated to a status of “Killed” (if status was InActive) or all the session lines will disappear altogether (if status was Active). In addition, the Message field will reflect the results of the mass kill action.

Figure 2.32. Figure.

Supply System User Administration

UserAccountName LastName FirstName MiddleInitial
MXIL2SMC CLANTON SPENCER M

User Sessions

SID	Serial#	Status	CurrentAction	LoginTime	Machine	Terminal	OSUser	OSPID	OSCommand
0012	02335	KILLED	UNKNOWN	26-MAR 10:28:56	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1388	1260
0013	02787	KILLED	UNKNOWN	26-MAR 10:29:25	GUNTER-2KWSSWDMS0035OUDR	WSSWDMS0035OUDR	Porteroa	1424	1224

KillAllSessions KillSelectedSession Cancel

Message: Killed All User Sessions for User MXIL2SMC

2.19.6. Screen 5 – Delete User.

Figure 2.33. Form Layout.

Supply System User Administration

UserAccountName LastName FirstName MiddleInitial

ConfirmDelete Cancel

Message:

2.19.6.1. The Delete User screen contains seven fields/action buttons and is accessed from the User/Data/Admin Actions screen (Screen 2).

2.19.6.2. User Identification section displays the following information:

User Account Name

Last Name

First Name

Middle Initial

2.19.6.3. The ConfirmDelete action button attempts an actual user deletion. The Cancel action button displays the User Data/Admin Actions screen. Message output field displays pertinent messages. Text in this field will vary from text saying the user was deleted to text saying the user was unable to be deleted and why.

2.19.7. Form Use.

Figure 2.34. Figure.

The screenshot shows a web application window titled "Supply System User Administration". It contains a table with the following data:

UserAccountName	LastName	FirstName	MiddleInitial
MX1L2SMC	CLANTON	SPENCER	M

Below the table are two buttons: "ConfirmDelete" and "Cancel". At the bottom, there is a "Message:" label followed by an empty text input field.

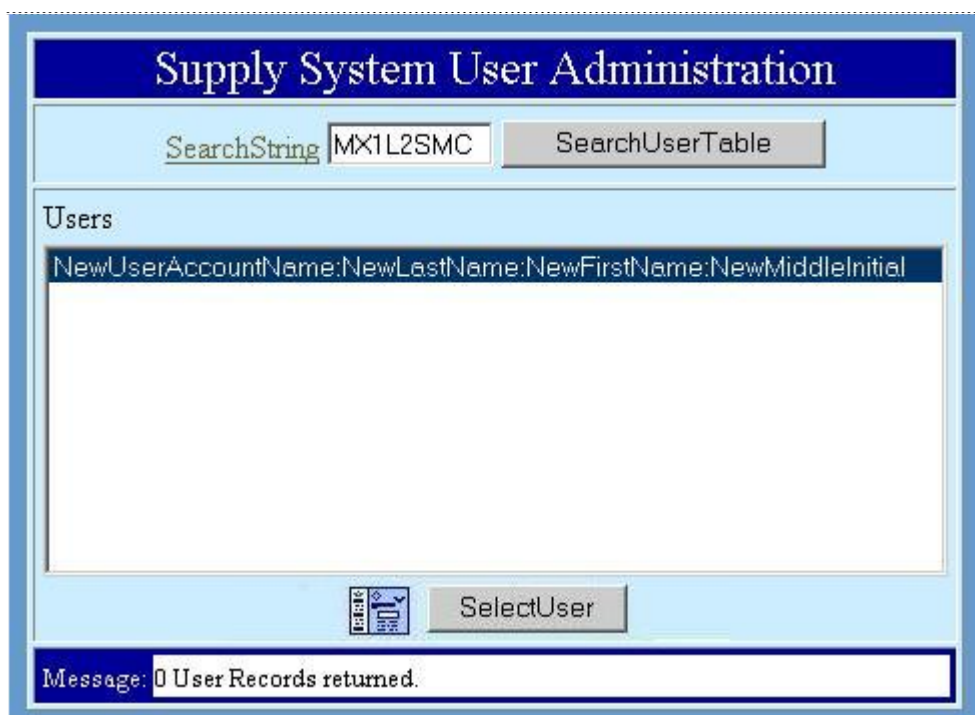
2.19.7.1. The ConfirmDelete action button is used to request deletion of a user account. The screen will be refreshed and the deletion is attempted. If the user account deletion fails for some reason then the Message field will state so. In addition, the screen will no longer contain the ConfirmDelete button. The Cancel button returns you to the User Data/Admin Actions screen.

Figure 2.35. Figure.

The screenshot shows the same web application window as Figure 2.34, but with a message displayed in the "Message:" field: "Deleted User MX1L2SMC". The "ConfirmDelete" and "Cancel" buttons are still present.

2.19.7.2. The Message field states the account was deleted when successful. This will only be displayed for a short period, then the Search/Select user screen will be displayed containing prior search criteria. A listing of matching users (minus the one that was just deleted) will be displayed.

Figure 2.36. Screen Image.



Supply System User Administration

SearchString SearchUserTable

Users

NewUserName:NewLastName:NewFirstName:NewMiddleInitial

SelectUser

Message: 0 User Records returned.